Message

From: Edward Cunningham [redacted]@google.com]
Sent: 8/15/2018 3:31:04 PM
To: Sameer Samat [redacted]@google.com]
CC: Jason Woloz [redacted]@google.com]; Jamie Rosenberg [redacted]@google.com]; Benjamin Poiesz [redacted]@google.com]; Mike Hochberg [redacted]@google.com]; Khawaja Shams [redacted]@google.com]; Tian Lim [redacted]@google.com]; Dave Kleidermacher [redacted]@google.com]; Sebastian Porst [redacted]@google.com]; Hiroshi Lockheimer [redacted]@google.com]; Colin Smith [redacted]@google.com]; Tristan Ostrowski [redacted]@google.com]; Kylie McRoberts [redacted]@google.com]; Salvador Mandujano [redacted]@google.com]; Shannon Newberry [redacted]@google.com]; Megan Johnston [redacted]@google.com]; Purnima Kochikar [redacted]@google.com]; Lydia Ash [redacted]@google.com]; Aaron Stein [redacted]@google.com]
Subject: Re: FN Update

The bug is not public. It is in the public issue tracker so could be made public (hence the big yellow warning). It is in a new restricted component, so only those directly CC'd can see it (ie. restricted to Epic Games).

We won't make public until they fix.

On Wed, Aug 15, 2018 at 4:29 PM, Sameer Samat [redacted]@google.com> wrote:
Thanks. Is it supposed to be public?

On Wed, Aug 15, 2018, 8:25 AM Jason Woloz [redacted]@google.com> wrote:
+ steina
Now that the bug is public
https://b.corp.google.com/issues/112630336

Colin or Aaron,
Is PR tracking press pickup?

On Mon, Aug 13, 2018 at 11:46 AM Sameer Samat [redacted]@google.com> wrote:
+ Lydia

On Mon, Aug 13, 2018, 9:24 AM Jason Woloz [redacted]@google.com> wrote:
For reference- We are tracking a newly form WG around Fortnite here

On Mon, Aug 13, 2018 at 8:59 AM Jamie Rosenberg [redacted]@google.com> wrote:
PRIVILEGED & CONFIDENTIAL

We're setting up an internal discussion for this morning to discuss next steps -- lots of pieces to coordinate (PR, partners, Epic, etc.), so pls continue to investigate but hold off on any actions/ comms until we have a chance to meet.

Re: Orange, they have their own app store (and have for a while). The discussion on Alley Oop was in the context of Android One, where we don't have third-party app stores and so were looking at ways that they could still merchandise in their app center but use Play for fulfillment.

On Mon, Aug 13, 2018 at 8:45 AM Benjamin Poiesz [redacted]@google.com> wrote:

Not aware of anything with Orange. INSTALL_PACKAGES doesn't currently go through the runtime permissions process, though there is a proposal for Q that it should (including all privileged permissions).

Ben

On Mon, Aug 13, 2018 at 8:37 AM Mike Hochberg [redacted]@google.com> wrote:
+Khawaja Shams

On Mon, Aug 13, 2018 at 8:35 AM Sameer Samat [redacted]@google.com> wrote:
I was not aware of that. Adding benp here who often handles oem preload request.

On Mon, Aug 13, 2018, 8:26 AM Tian Lim [redacted]@google.com> wrote:
this is really good work.

i see the orange app center is afforded the same special treatment by samsung - 2 questions
1) (not asking you to do this work) have you done a similar analysis of the orange app installer?
2) more broadly to jamie/sameer - i remember there being an escalation around orange and how they'd build an app store with alley oop. did we know/care about this samsung deal?

thx

On Mon, Aug 13, 2018 at 8:18 AM Jamie Rosenberg [redacted]@google.com> wrote:
Very interesting...and concerning.

I'll set up a meeting for a few of us today to discuss.

On Mon, Aug 13, 2018, 8:03 AM Edward Cunningham [redacted]@google.com> wrote:
I took a deeper look on Friday and discovered a vulnerability in the Fortnite Installer (and Galaxy Apps private installer API) which allows a malicious app to install a fake version of Fortnite with arbitrary permissions auto-granted.

I wrote up my findings in this doc, and did a screen recording demo here.

Not exactly sure what we should do with this, but we should inform Epic probably. (A Project Zero style external bug would be the most fun!)

On Thu, Aug 9, 2018 at 7:15 PM, Edward Cunningham [redacted]@google.com> wrote:
Based on GPP logs, I have confirmed for certain that the app which actually performs the installation of the main Fortnite game is com.sec.android.app.samsungapps.

The logs also show a few instances of a Pixel installing the main Fortnite game via unknown sources from the official Fortnite Installer, so I can only assume that this was a test of the non-Samsung install flow (happening just as we expect).

On Thu, Aug 9, 2018 at 5:32 PM, Dave Kleidermacher [redacted]@google.com> wrote:
I have a loaner S8 and will bring it around later in MTV if anyone wants it...

On Thu, Aug 9, 2018 at 9:30 AM Edward Cunningham [redacted]@google.com> wrote:
So far the install flows I have seen in the APK are as follows:

1. Fortnite Installer self-update (via unknown sources). If you have an old Fortnite Installer installed, it prompts you to grant unknown sources and then downloads/installs an update to itself.

2. Main game install via Samsung Apps private API. This is why on Samsung devices it doesn't need unknown sources to be enabled. The Fortnite Installer itself downloads the APK, and then uses Samsung Apps to do the install in the background. I imagine Samsung maintains a whitelist of who is able to do this (otherwise this itself will be an exciting security vulnerability).

I haven't completely figured out the part of the code where they install the game on non-Samsung devices (of course it is possible that code isn't included yet).

On Thu, Aug 9, 2018 at 5:18 PM, Sameer Samat [redacted]@google.com> wrote:
Well. That seems quite bad. You are seeing this fornite thing on other devices besides Samsung devices?!

On Thu, Aug 9, 2018, 9:13 AM Sebastian Porst [redacted]@google.com> wrote:
+Edward Cunningham

Hi all,

on Samsung devices the installer seems to use something called the Samsung Installer Service. On non-Samsung devices they seem to ask for unknown sources to be enabled. Added Edward who played around with this.

Sebastian

On Thu, Aug 9, 2018 at 9:00 AM Dave Kleidermacher [redacted]@google.com> wrote:
Privileged & Confidential

Samsung store has install apps permission, so perhaps the Epic installer is leveraging that, e.g. via a Samsung API vs. doing a direct install on its own. That would be a clever way for them to avoid the unknown sources friction entirely. Adding GPP leads to investigate.

On Thu, Aug 9, 2018 at 8:50 AM Sameer Samat [redacted]@google.com> wrote:
+Tian Lim +Mike Hochberg, +Dave Kleidermacher

*** attorney client privileged ***
*** seeks advice of counsel

Opened my note8 today, went to galaxy apps, saw fornite banner so I gave it a try. Here is the flow.

Main point: Something is wrong. The Epic installer never asked me to turn on US. In fact, I checked after it was done and it did not have the permission. But it was able to download and install Fornite. I have Fortnite now on my Note8 running. ?!

Obvious things wrong here:

* Note8? I thought this was a note9 thing. Maybe this is going to many samsung devices today?
* Epic installer does not have unknown sources, but somehow is able to download and install fortnite.

* The epic installer is hosted in the samsung galaxy store. It's not a link out to some website (I think they conveyed this change last night)

On Wed, Aug 8, 2018 at 7:13 PM Jamie Rosenberg [redacted]@google.com> wrote:
Privileged

Correct. It's always been part of Epic's plan to have the installer apk -- to manage updates, etc. (Similar to what Facebook does). So the user was always going to have to download two apks.

The new info is that Samsung will host and deliver the installer apk, removing the need for US prompts for that one.

Am double confirming that US will still be required for the installer apk to facilitate the download of the game.

On Wed, Aug 8, 2018 at 7:11 PM Sameer Samat [redacted]@google.com> wrote:
**** attorney client privileged ***
*** seeks advice of counsel ***

Sorry for being slow -- not sure I follow -- you go to the samsung store and tap "fornite!", it starts downloading the epic installer (e.g. the samsung store installs the epic installer). Then when you run the epic installer you need to give it US permission -- then it installs FN?

On Wed, Aug 8, 2018 at 7:07 PM Hiroshi Lockheimer [redacted]@google.com> wrote:
PRIVILEGED

Yep exactly

On Thu, Aug 9, 2018 at 11:06 AM Jamie Rosenberg [redacted]@google.com> wrote:
PRIVILEGED

Which parts would you like clarification on? They said that the installer APK would not be preloaded and would be a user-initiated download, managed by Samsung -- and so no unknown sources prompt.

And the delivery of the game would be managed by the installer. Are you wanting to confirm that they haven't somehow given the installer permission to bypass the unknown sources prompt?

On Wed, Aug 8, 2018 at 7:01 PM Hiroshi Lockheimer [redacted]@google.com> wrote:

PRIVILEGED

Can we please get a definitive answer on the end to end user flow? Samsung should be able to provide us that .

On Thu, Aug 9, 2018, 10:54 AM Jamie Rosenberg [redacted]@google.com> wrote:
ATTORNEY CLIENT PRIVILEGED

(Tristan, please advise)

FYI, a few more details from Samsung on the user flows related to Fortnite on Note 9.

* From both Galaxy Apps and the Samsung Games Launcher app, there will be a pormo/ link to install Fortnite
* Samsung will host and deliver the Fortnite installer apk (likely as a privileged install -- no unknown sources)
* The Fortnite installer apk will then prompt the user to download the game from Epic (presumably requiring the unknown sources prompt)

Apparently Samsung asked Epic to be able to host the game in Galaxy Apps and it was Epic's preference to host on their side.

--
BR,
Dave

Dave Kleidermacher
VP, Head of Security - Android, Chrome OS, Play

--
BR,
Dave

Dave Kleidermacher
VP, Head of Security - Android, Chrome OS, Play

--
Be well,
Jason

Jason Woloz | Android Security [redacted]@google.com

--
Be well,
Jason

Jason Woloz | Android Security | [redacted]@google.com